



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/804,511	03/12/2001	Gen Ichimura	7217/64035	1971

7590 10/12/2004

Jay H. Maioli
Cooper & Dunham LLP
1185 Avenue of the Americas
New York, NY 10036

EXAMINER

TRUONG, THANHNGA B

ART UNIT	PAPER NUMBER
----------	--------------

2135

DATE MAILED: 10/12/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

3

Office Action Summary

Application No.

09/804,511

Applicant(s)

ICHIMURA, GEN

Examiner

Thanhnga Truong

Art Unit

2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 12 March 2001.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-41 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-41 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 12 March 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some * c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____

DETAILED ACTION

Claim Rejections - 35 USC § 112

1. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

2. Claims 20 and 24 recite the limitation "variable" on pages 66 and 67. Claims 29, 30, 40, and 41 recite the limitation "unencrypted data" on pages 69, 71, and 72. There is insufficient antecedent basis for these limitations in the claims.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 17-20, 25 are rejected under 35 U.S.C. 102(e) as being anticipated by Tatebayashi et al.

a. *Referring to claim 17:*

- i. Tatebayashi teaches:

(1) random-data-generating means for generating random data [i.e., referring to Figure 1, the message generation unit 106 can be realized by a random number generator that generates a random number and stores it as the message M (column 4, lines 26-28)];

(2) addition means for adding said random data generated by said random-data-generating means to the beginning and the end of said program [i.e., referring to Figure 1, "adding random data" is considered to include

in the message generation unit 106 which can be realized by a random number generator (column 4, lines 26-27)];

(3) encryption-processing means for encrypting said program including said random data added thereto by said addition means [i.e., referring to Figure 1, the encryption module 102 can be an integrated circuit (IC) that performs encryption based on a secret encryption algorithm E1 (column 4, lines 10-12)]; and

(4) transmission means for transmitting said program encrypted by said encryption-processing means [i.e., referring to Figure 1 again, the transmission units 110, 111, and 112 can each be composed of a parallel-to-series convertor and an amplifier, and are respectively used to transmit the cryptograms Cd, Ca, and Cm to the reception apparatus 200 via the transfer paths 120, 121, and 122 (column 4, lines 51-55)].

b. Referring to claim 18:

i. Tatebayashi further teaches:

(1) wherein said transmission means transmits said encrypted digital data to other equipment by radio or wire communication [i. e., referring to Figure 1, the transfer paths 120-122 can be composed of communication cables or a recording medium (column 4, lines 56-57)].

c. Referring to claim 19:

i. Tatebayashi further teaches:

(1) wherein said transmission means transmits said encrypted digital data as data to be recorded onto a recording medium [i. e., referring to Figure 1, the transfer paths 120-122 can be composed of communication cables or a recording medium (column 4, lines 56-57)].

d. Referring to claim 20:

i. Tatebayashi further teaches:

(1) wherein the data length of said random data generated by said random-data-generating means is variable [i.e., referring to Figure 1, the message generation unit 106 can be realized by a random number

generator that generates a random number, that is "variable", and stores it as the message M (column 4, lines 26-28)].

e. Referring to claim 25:

i. This claim has limitations that is similar to those of claim 17, thus it is rejected with the same rationale applied against claim 17 above.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

6. Claims 1-6, 13-14, 27-35, 36-41 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tatebayashi et al (US 6, 009, 174), and further in view of Wasilewski (US 5, 420, 866).

a. Referring to claim 1:

i. Tatebayashi teaches:

(1) insertion means for inserting random data into a part of said packet-converted digital data to be transmitted [**i.e., referring to Figure 1, the message generation unit 106 can be realized by a random number generator that generates a random number and stores it as the message M (column 4, lines 26-28)];**

(2) encryption means for encrypting said packet-converted digital data including said random data inserted by said insertion means [**i.e., referring to Figure 1, the encryption module 102 can be an integrated circuit (IC) that performs encryption based on a secret encryption algorithm E1. The encryption module 102 reads a one-block unit of the digital data "Data" from the digital production 101, encrypts the data using the secret key Ks sent from the secret key selection unit 104 as the encryption key, and transfers the obtained cryptogram Cd(=E1(Data,Ks)) to the transmission unit 110. The encryption**

module 102 repeats this processing for all of the data in the digital production 101 (column 4, lines 10-19). Furthermore, the encryption module 105 can be an integrated circuit (IC) that performs encryption based on a secret encryption algorithm E2. The encryption module 105 reads the message M stored in the message generation unit 106, encrypts it using the secret key Ks sent from the secret key selection unit 104 as the encryption key, and transfers the obtained cryptogram $C_a(=E_2(M, K_s))$ to the transmission unit 111. The encryption module 107 can be an integrated circuit (IC) that performs encryption based on a secret encryption algorithm E3. The encryption module 107 reads the message M stored in the message generation unit 106, encrypts it using the message M itself as the encryption key, and transfers the obtained cryptogram $C_m(=E_3(M, M))$ to the transmission unit 112 (column 4, lines 33-46)]; and

(3) transmission means for transmitting said digital data encrypted by said encryption means [i.e., referring to Figure 1 again, the transmission units 110, 111, and 112 can each be composed of a parallel-to-series convertor and an amplifier, and are respectively used to transmit the cryptograms C_d , C_a , and C_m to the reception apparatus 200 via the transfer paths 120, 121, and 122 (column 4, lines 51-55)].

ii. Although, Tatebayashi has mentioned the used of digital data in his invention, he, however, does not clearly express:

(1) inserting data into a part of said packet-converted digital data.

iii. Whereas, Wasilewski teaches:

(1) Wasilewski's invention is directed to methods for providing conditional access information to decoders in a packet-based multiplexed communications system wherein a plurality of different elementary streams are each segmented and inserted into respective transport packets that are then multiplexed to form a single transport stream for transmission to a remote location (column 5, lines 31-37).

iv. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) clearly express the used of digital data in a packet-based multiplexed communication systems (in Tatebayashi) in order to provide conditional access information to decoders in the system (**column 7, lines 62-63 of Wasilewski**).

v. The ordinary skilled person would have been motivated to:

(1) clearly express the used of digital data in a packet-based multiplexed communication systems (in Tatebayashi) for providing a plurality of different sets of conditional access information to a remote location and for facilitating access to a selected one of those sets of conditional access information by a decoder at the remote location (**column 5, lines 39-43 of Wasilewski**).

b. Referring to claim 2:

i. Tatebayashi further teaches:

(1) wherein said transmission means transmits said encrypted digital data to other equipment by radio or wire communication [**i. e., referring to Figure 1, the transfer paths 120-122 can be composed of communication cables or a recording medium (column 4, lines 56-57)**].

c. Referring to claim 3:

i. Tatebayashi further teaches:

(1) wherein said transmission means transmits said encrypted digital data as data to be recorded onto a recording medium [**i. e., referring to Figure 1, the transfer paths 120-122 can be composed of communication cables or a recording medium (column 4, lines 56-57)**].

d. Referring to claim 4:

i. Wasilewski further teaches:

(1) wherein said insertion means inserts said random data into an invalid-data portion existing in said packet [**i.e., referring to Figures 7A-7B, "invalid-data portion" is considered to be part of the respective sequence of transport packets (column 5, lines 45-51)**].

e. Referring to claim 5:

i. Wasilewski further teaches:

(1) wherein the length of an encryption unit encrypted by said encryption means is smaller than the length of said packet-converted digital data **[i.e., referring to Figure 3B, the encryption related information is only one part of the elementary stream (column 6, lines 23-26)].**

f. Referring to claim 6:

i. This claim has limitations that is similar to those of claim 1, thus it is rejected with the same rationale applied against claim 1 above.

g. Referring to claims 13, 27, 34:

i. These claims have limitations that is similar to those of claim 1, thus they are rejected with the same rationale applied against claim 1 above.

h. Referring to claim 14:

i. This claim has limitations that is similar to those of claims 5-6, thus it is rejected with the same rationale applied against claims 5-6 above.

i. Referring to claims 28-30, 35:

i. These claims have limitations that is similar to those of claim 1, thus they are rejected with the same rationale applied against claim 1 above.

g. Referring to claim 31:

i. This claim has limitations that is similar to those of claim 4, thus it is rejected with the same rationale applied against claim 4 above.

g. Referring to claim 32:

i. This claim has limitations that is similar to those of claim 2, thus it is rejected with the same rationale applied against claim 2 above.

g. Referring to claim 33:

i. This claim has limitations that is similar to those of claim 3, thus it is rejected with the same rationale applied against claim 3 above.

i. Referring to claims 36-41:

i. These claims have limitations that is similar to those of claims 1 and 3, thus they are rejected with the same rationale applied against claims 1 and 3 above.

7. Claims 7-12, 15-16, 21-24, 26, are rejected under 35 U.S.C. 103(a) as being unpatentable over Tatebayashi et al (US 6, 009, 174), and further in view of Wasilewski (US 5, 420, 866) and Holtz (US 5, 917, 948).

a. Referring to claim 7:

i. Tatebayashi teaches:

(1) reception means for receiving encrypted packet-converted digital data [i.e., referring to **Figure 1**, the reception units 210, 211, and 212 can each be composed of a series-to-parallel convertor, and are respectively used to receive the three kinds of cryptogram Cd, Ca, and Cm from the transfer paths 120, 121, and 122 (column 5, lines 5-8)];

(2) decryption means for decrypting said encrypted packet-converted digital data received by said reception means [i.e., the decryption module 201 can be composed of an IC for performing decryption based on the secret decryption algorithm D1 that is the inverse transformation of the encryption algorithm E1 of the encryption module 102 in the transmission apparatus 100. When given a secret key Ks by the secret key selection unit 202, the decryption module 201 uses the secret key to decrypt the cryptogram Cd sent from the reception unit 210, and by doing so restores the block data "Data" (=D1(Cd,Ks)) of the original digital production (column 5, lines 9-17)]; and

ii. Although, Tatebayashi has mentioned the used of digital data in his invention, he, however, does not clearly express:

(1) packet-converted digital data.

iii. Whereas, Wasilewski teaches:

(1) Wasilewski's invention is directed to methods for providing conditional access information to decoders in a packet-based multiplexed communications system wherein a plurality of different elementary streams are each

segmented and inserted into respective transport packets that are then multiplexed to form a single transport stream for transmission to a remote location (**column 5, lines 31-37**).

iv. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) clearly express the used of digital data in a packet-based multiplexed communication systems (in Tatebayashi) in order to provide conditional access information to decoders in the system (**column 7, lines 62-63 of Wasilewski**).

v. The ordinary skilled person would have been motivated to:

(1) clearly express the used of digital data in a packet-based multiplexed communication systems (in Tatebayashi) for providing a plurality of different sets of conditional access information to a remote location and for facilitating access to a selected one of those sets of conditional access information by a decoder at the remote location (**column 5, lines 39-43 of Wasilewski**).

vi. Eventhough, Tatebayashi does not explicitly mention:

(1) elimination means for removing random data from packet-converted digital data obtained as a result of decryption carried out by said decryption means.

vii. Holtz teaches:

(1) Since random noise is interpreted as "movement" any increase in noise will increase the transmission bandwidth. Removing noise from the images before transmission will not only improve the image quality but may lead to cheaper transmissions (**column 18, line 66 through column 19, line 4**).

viii. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) include random noise (in message generation unit M of Tatebayashi) to control a better quality reception of digital data/image.

xi. The ordinary skilled person would have been motivated to:

(1) include random noise (in message generation unit M of Tatebayashi) to improve the digital data/image quality.

b. Referring to claims 8, 22:

i. These claims have limitations that is similar to those of claim 2, thus they are rejected with the same rationale applied against claim 2 above.

c. Referring to claims 9, 23:

i. These claims have limitations that is similar to those of claim 3, thus they are rejected with the same rationale applied against claim 3 above.

d. Referring to claim 10:

i. This claim has limitations that is similar to those of claim 7, thus it is rejected with the same rationale applied against claim 7 above.

e. Referring to claim 11:

i. This claim has limitations that is similar to those of claim 5, thus it is rejected with the same rationale applied against claim 5 above.

f. Referring to claim 12:

i. Tatebayashi further teaches:

(1) wherein said elimination means eliminates said random data from said decryption unit [i.e., referring to Figure 1, “eliminates random data” is considered to include in decryption module 201].

g. Referring to claims 15, 21, 26:

i. These claims have limitations that is similar to those of claim 7, thus they are rejected with the same rationale applied against claim 7 above.

h. Referring to claim 16:

i. This claim has limitations that is similar to those of claims 11-12, thus it is rejected with the same rationale applied against claims 11-12 above.

i. Referring to claim 24:

i. Tatebayashi further teaches:

(1) wherein the data length of said random data generated by said random-data-generating means is variable [i.e., referring to Figure 1, the message generation unit 106 can be realized by a random number

generator that generates a random number, that is "variable", and stores it as the message M (column 4, lines 26-28)].

Conclusion

8. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Kubota et al (US 5, 721, 778) discloses a digital signal transmitting method, a digital signal receiving apparatus, and a recording medium which ensure the security of fee-charged software information (see abstract).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thanhnga (Tanya) Truong whose telephone number is 703-305-0327.

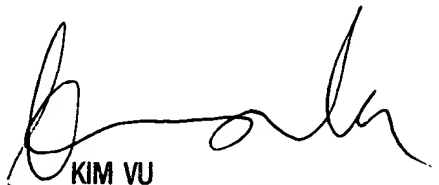
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached at 703-305-4393. The fax and phone numbers for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

TC 2100 will be moved to Carlyle in October 2004, the new telephone number for TC 2100 receptionist is 571-272-2100. In October 2004, any inquiry concerning this communication should be directed to Thanhnga (Tanya) Truong whose new telephone number is 571-272-3858, and the examiner's supervisor, Kim Vu can be reached at 571-272-3859.

TBT

September 9, 2004


KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100